

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平8-84140

(43)公開日 平成8年(1996)3月26日

(51)Int.Cl.⁶ 識別記号 庁内整理番号 F I 技術表示箇所
H 04 L 9/00
9/10
9/12
H 04 M 3/42 E H 04 L 9/00 Z
審査請求 未請求 請求項の数 4 OL (全 11 頁)

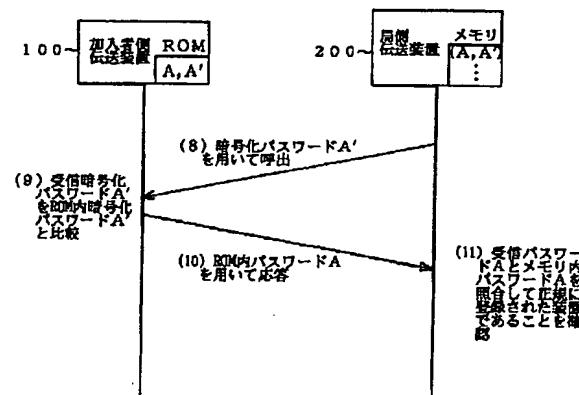
(21)出願番号	特願平6-217009	(71)出願人	000004226 日本電信電話株式会社 東京都新宿区西新宿三丁目19番2号
(22)出願日	平成6年(1994)9月12日	(72)発明者	三鬼 準基 東京都千代田区内幸町1丁目1番6号 日本電信電話株式会社内

(54)【発明の名称】 加入者認証方法

(57)【要約】

【目的】 安全性が高くかつ所要回路規模の少ない加入者認証を実現する。

【構成】 複数の加入者側装置100が通信網を介して局側装置200と結ばれ、局側装置は登録された加入者側装置にサービスを提供する。加入者側装置100は、装置固有のパスワードAと該パスワードAを公開鍵で暗号化した暗号パスワードA'を保持し、そのうち、暗号パスワードA'を局側装置200に登録する。局側装置200は、各加入者側装置毎に、暗号パスワードA'とそれを秘密鍵で復号したパスワードAを保持する。通信の開始時、局側装置200はA'を用いて通信相手の加入者側装置100を呼び出し、加入者側装置100は、受信したA'を自己のA'を比較し、一致するとAで応答し、局側装置200は、受信したAを保持してあるAと照合する。



1

【特許請求の範囲】

【請求項1】複数の加入者側伝送装置が通信ネットワークを介して局側伝送装置と結ばれ、局側伝送装置は登録された加入者側伝送装置にサービスを実施する登録加入者通信サービスシステムにおいて、加入者側伝送装置が局側伝送装置に正規に登録された装置であることを確認する加入者認証方法であって、

加入者側伝送装置は、各々、加入者側伝送装置を識別するための装置固有の秘密情報とネットワーク事業者から割り当てられた公開鍵で前記秘密情報を暗号化した暗号化情報とを保持するとともに、前記暗号化情報を局側伝送装置に登録し、

局側伝送装置は、各加入者側伝送装置について、加入者側伝送装置からの暗号化情報と該暗号化情報を秘密鍵により復号した復号情報を組として保持し、

通信の開始時に、局側伝送装置は通信相手の加入者側伝送装置の暗号化情報を用いて加入者側伝送装置を呼び出し、加入者側伝送装置は局側伝送装置からの暗号化情報と自己の暗号化情報を比較して、一致する場合に自己の秘密情報を用いて応答し、局側伝送装置は加入者側伝送装置から送られてきた秘密情報を保持している復号情報を照合することにより、通信相手の加入者側伝送装置が正規に登録された装置であることを確認することを特徴とする加入者認証方法。

【請求項2】加入者側伝送装置の装置固有の秘密情報と、ネットワーク事業者から割り当てられた公開鍵で前記秘密情報を暗号化した暗号化情報を組として、あらかじめ装置製造時または出荷時に個々の加入者側伝送装置内の読み出し専用記憶素子(ROM)に書き込んでおくことを特徴とする請求項1に記載の加入者認証方法。

【請求項3】加入者側伝送装置はネットワーク事業者から割り当てられたID番号を設定する手段を有し、加入者側伝送装置の設置時に、局側伝送装置はID番号を用いて加入者側伝送装置の呼び出しを行い、加入者側伝送装置は局側伝送装置からのID番号と自己のID番号とを比較し、一致する場合、自己の暗号化情報を局側伝送装置へ送信して登録することを特徴とする請求項1に記載の加入者認証方法。

【請求項4】通信の開始時に、局側伝送装置は通信相手の加入者側伝送装置の暗号化情報の一部あるいは全て、および局側伝送装置にあらかじめ登録したID番号を用いて加入者側伝送装置を呼び出し、加入者側伝送装置は局側伝送装置からの暗号化情報の一部あるいは全ておよびID番号と自己の暗号化情報およびID番号についてそれぞれ比較を行い、一致する場合に自己の秘密情報を用いて応答することを特徴とする請求項3に記載の加入者認証方法。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、一つの局側伝送装置と 50

2

複数の加入者側伝送装置が対向するポイント・ツー・マルチポイント形態の登録加入者通信サービスシステムにおける加入者認証方法に関するものである。

【0002】

【従来の技術】図8は登録加入者通信サービスシステムの概略構成を示したもので、100は加入者側伝送装置、200は局側伝送装置、300はネットワークオペレーションシステム、400は加入者側伝送装置100と局側伝送装置200の間に介在するネットワーク網である。ネットワークオペレーションシステム300は、加入者からの申告などによりサービスを許可する加入者側伝送装置100を局側伝送装置200に登録し、局側伝送装置200は、この正規に登録された加入者側伝送装置100に対して所望のサービスを実施する。なお、ネットワークオペレーションシステム300は一般には複数の局側伝送装置を収容し、各局側伝送装置にそれぞれ複数の加入者側伝送装置がポイント・ツー・マルチポイント形態で接続されて、それぞれサービスエリアを形成している。

【0003】従来、この種登録加入者通信サービスシステムにおける加入者認証方法は、個々の加入者側伝送装置に、その装置を識別するためのID番号と正規に登録された装置であることを証明するためのパスワードを割り当て、加入者側伝送装置に内蔵されたROM(Read Only Memory)とネットワーク事業者の所有するデータベースに書き込む方式を探っていた。図6および図7により、従来の加入者認証手順の例を説明する。

【0004】図6は登録時の手順を示したもので、まず、ネットワーク事業者がID番号とパスワードの対を大量に生成し(1)、データベースに蓄積する(2)。次に、これを伝送装置の製造業者に知らせる(3)。製造業者は装置の製造時または出荷時に個々の加入者側伝送装置のROMにID番号とパスワードを1組書き込む(4)。加入者は、加入者側伝送装置を購入した後(5)、その装置のID番号をネットワークオペレーションシステムに登録する(6)。これは、通常は加入者が自伝送装置のID番号をネットワーク事業者に届けることで行われる。ネットワークオペレーションシステムは、登録されたID番号を元にデータベースの検索を行い(7)、対応するパスワードを読み出し(8)、局側伝送装置のメモリに、これらのID番号とパスワードを書き込む(9)。

【0005】通信の開始時には、図7に示すように、毎回、局側伝送装置がID番号を用いて加入者側伝送装置を呼び出し(10)、加入者側伝送装置はパスワードを用いて応答する(11)。局側伝送装置は、メモリに記憶されているパスワードと受信したパスワードを照合することで、正規に登録された伝送装置であることを確認する(12)。

【0006】

【発明が解決しようとする課題】上記従来の加入者認証方法では、大量のID番号とパスワードを書き込むための大規模なデータベースを必要する問題がある。また、加入者側伝送装置、局側伝送装置、ネットワークオペレーションシステム、及びデータベースの各装置間の伝送は安全性が保証されている必要があるため、伝送装置は暗号化回路等の付加により回路規模が増大するという問題もある。

【0007】本発明は、大規模なデータベースを必要とせず、なおかつ伝送装置の回路規模が少なくてすむ加入者認証方法を提供することにある。

【0008】

【課題を解決するための手段】本発明の加入者認証方法は、各加入者側伝送装置は、加入者側伝送装置を識別するための装置固有の秘密情報（パスワード）Aとネットワーク事業者から割り当てられた公開鍵Pで前記秘密情報Aを暗号化した暗号化情報A'を保持するとともに、前記暗号化情報A'を局側伝送装置に登録し、局側伝送装置は、各加入者側伝送装置について、加入者側伝送装置からの暗号化情報A'を復号する。この暗号化情報A'を秘密鍵Qにより復号した復号情報Aと組として保持し、通信の開始時に、局側伝送装置は通信相手の加入者側伝送装置の暗号化情報A'を用いて加入者側伝送装置を呼び出し、加入者側伝送装置は局側伝送装置からの暗号化情報A'を復号する。この暗号化情報A'と自己の暗号化情報A'を比較して、一致する場合に自己の秘密情報Aを用いて応答し、局側伝送装置は加入者側伝送装置から送られてきた秘密情報Aを保持されている復号情報Aと照合することにより、通信相手の加入者側伝送装置が正規に登録された装置であることを確認することを特徴とする。

【0009】また、本発明の加入者認証方法は、加入者側伝送装置の装置固有の秘密情報Aと、ネットワーク事業者から割り当てられた公開鍵Pで前記秘密情報Aを暗号化した暗号化情報A'を組として、あらかじめ装置製造時または出荷時に個々の加入者側伝送装置内の読み出し専用記憶素子（ROM）に書き込んでおくことを特徴とする。

【0010】また、本発明の加入者認証方法は、加入者側伝送装置はネットワーク事業者から割り当てられたID番号を設定する手段を有し、加入者側伝送装置の設置時に、局側伝送装置はID番号を用いて加入者側伝送装置の呼び出しを行い、加入者側伝送装置は局側伝送装置からのID番号と自己のID番号とを比較し、一致する場合、自己の暗号化情報A'を局側伝送装置へ送信して登録することを特徴とする。

【0011】更には、本発明の加入者認証方法は、通信の開始時に、局側伝送装置は通信相手の加入者側伝送装置の暗号化情報A'の一部あるいは全て、および局側伝送装置にあらかじめ登録した上記ID番号を用いて加入者側伝送装置を呼び出し、加入者側伝送装置は局側伝送

装置からの暗号化情報A'の一部あるいは全ておよびID番号と自己の暗号化情報A'およびID番号についてそれぞれ比較を行い、一致する場合に自己の秘密情報Aを用いて応答することを特徴とする。

【0012】

【作用】本発明は、公開鍵暗号方式の一方向性を利用して、製造業者に割り当てた公開鍵と暗号化された秘密情報（暗号化されたパスワード）だけでは元の秘密情報（パスワード）を解読できないことを保証しつつ、伝送装置自体には秘密情報（パスワード）の暗号化／復号化回路を不要にするものである。

【0013】公開鍵暗号方式を用いた暗号化は、通常、図9に示す様な形態で実施される。秘密情報（パスワード）Aを公開鍵Pにより暗号化を行い、該暗号化情報A'を安全でない伝送路を経由して送信する。暗号化情報A'を受け取った側は、秘密鍵Qを用いて元の秘密情報（パスワード）Aを復号する。この公開鍵暗号方式の特徴は、暗号化情報A'と公開鍵Pからは元の秘密情報Aを解読することはできないということである。

20 【0014】本発明では、この公開鍵暗号化方式を利用することにより、IDとパスワードを予め記憶しておくための大規模なデータベースを必要とせず、また、秘密情報及びその暗号化情報をあらかじめ伝送装置に保持しておくことにより、伝送装置自体には秘密情報の暗号化／復号化回路は不要である。

【0015】

【実施例】以下、本発明の実施例について図面を参照して説明する。

【0016】（実施例1）これは請求項1および2に対応するものである。図1および図2により、本実施例の加入者認証手順を説明する。図1は登録時の手順を示したもので、まず、ネットワーク事業者は公開鍵Pとそれに対応する秘密鍵Qを生成する（1）。次に、秘密鍵Qはネットワークオペレーションシステム300に登録し（2）、公開鍵Pを伝送装置の製造業者に知らせる（3）。製造業者は装置の製造時または出荷時に、装置固有の秘密情報であるパスワードAを生成し、公開鍵Pを用いてこのパスワードAを暗号化する。そして、個々の加入者側伝送装置100のROMに、該装置固有のパスワードAとその暗号化情報である暗号化パスワードA'を1組書き込む（4）。加入者は加入者側伝送装置100を購入した後（5）、その装置の暗号化パスワードA'をネットワーク事業者に届け出て、ネットワークオペレーションシステム300に登録する（6）。ネットワークオペレーションシステム300は、登録された暗号化パスワードA'を秘密鍵Qを用いて元のパスワードAに復号した後、局側伝送装置200のメモリに、これら暗号化パスワードA'とその復号情報であるパスワードAを組にして書き込む（7）。

50 【0017】通信の開始時には、図2に示す様に毎回、

局側伝送装置200が暗号化パスワードA'を用いて通信相手の加入者側伝送装置100を呼び出す(8)。加入者側伝送装置100は局側伝送装置200からの暗号化パスワードA'を受信し、ROM内の自己の暗号化パスワードA'と比較を行い(9)、一致する場合は、局側伝送装置200に対してROM内の自己のパスワードAを用いて応答する(10)。一致しない場合は応答しない。局側伝送装置200は、メモリに記憶されている暗号化パスワードA'と対のパスワードAと受信したパスワードAを照合することで、正規に登録された加入者側伝送装置100であることを確認する(11)。

【0018】本実施例の認証手順を用いた場合、公開鍵暗号方式が安全である限り、暗号化パスワードA'と公開鍵Pだけでは元のパスワードAを復号できないため、加入者側伝送装置100のROMに書き込まれたパスワードAを盗み出されか、ネットワーク事業者の有する秘密鍵Qを盗み出さない限り、他の加入者になりますことはできない。また、ID番号とパスワードを予め記憶しておくための大規模なデータベースを必要とせず、伝送装置100, 200にも秘密情報(パスワード)の暗号化/復号化のための回路を必要としない。

【0019】(実施例2)これは請求項3および4に対応し、パスワードの登録を遠隔から自動的に行える様にするとともに、パスワードの安全性をさらに高めるものである。図3、図4および図5により、本実施例の加入者認証手順を説明する。

【0020】図3において、まず、ネットワーク事業者は公開鍵Pとそれに対応する秘密鍵Qを生成する

(1)。次に、秘密鍵Qはネットワークオペレーションシステム300に登録し(2)、公開鍵Pを伝送装置の製造業者に知らせる(3)。製造業者は伝送装置の製造時または出荷時に、装置固有の秘密情報であるパスワードAを生成し、公開鍵Pを用いてこのパスワードAを暗号化する。そして、個々の加入者側伝送装置100のROMに、該装置固有のパスワードAとその暗号化情報である暗号化パスワードA'を1組書き込む(4)。ここで、加入者側伝送装置100には、個々の加入者側伝送装置を区別するためのID番号を設定するスイッチ(数桁の数値を設定できるスイッチ)が具備されているとする。加入者は加入者側伝送装置100を購入した後(5)、ネットワーク事業者からID番号の割り当てを受け(6)、加入者側伝送装置100に設定する(7)。一方、ネットワーク事業者は、加入者に割り当てたID番号をネットワークオペレーションシステム300を経由して局側伝送装置200のメモリに登録する(8)。

【0021】図4は遠隔登録の手順を示したもので、加入者が加入者側伝送装置100をネットワークに接続した際、局側伝送装置200は、ID番号を用いて加入者側伝送装置100の呼出しを行う(9)。加入者側伝送

装置100は局側伝送装置200から受信したID番号を自己のID番号と比較を行い(10)、一致する場合はROM内の自己の暗号化パスワードA'を用いて応答する(11)。一致しない場合は応答しない。局側伝送装置200は、受信した暗号化パスワードA'をネットワークオペレーションシステム300に送る(12)。ネットワークオペレーションシステム300は秘密鍵Qを用いて、元のパスワードAを復号し(13)、局側伝送装置200に返す(14)。局側伝送装置200は、暗号化パスワードA'とその復号情報のパスワードAをIDと組にしてメモリに書き込む。

【0022】この様にして、本実施例では、ネットワーク事業者から割り当てられたID番号を設定した加入者側伝送装置をネットワークに接続するだけで自動的に加入者登録が行われる。

【0023】通信の開始時には、図5に示す様に、局側伝送装置200がID番号と暗号化パスワードA'の一部あるいは全てを組み合わせた値を用いて、加入者側伝送装置100を呼び出す(15)。加入者側伝送装置100は、局側伝送装置200からID番号および暗号化パスワードA'を受信して、スイッチに設定された自己的ID番号およびROM内の暗号化パスワードA'をそれぞれ比較し(16)、一致する場合はパスワードAを用いて応答する(17)。一致しない場合は応答しない。局側伝送装置200は、メモリに記憶されているパスワードAと受信したパスワードAを照合することで、正規に登録された加入者側伝送装置であることを確認する(18)。

【0024】既存の認証方式では、ID番号は、ネットワーク事業者がサービスを提供している全ての地域で加入者側伝送装置を一意に決定できる必要があったため、非常に多くの桁数が必要であった。本実施例では、加入者側伝送装置をネットワークに接続する最初の時に、そのローカルなネットワーク内で加入者側伝送装置を区別できれば良いため、ID番号は2~3桁程度で十分である。また、通信の開始時の加入者側伝送装置呼び出し時にID番号を併せて用いることにより、パスワードを一部のみ使用することが可能となるため、パスワードの安全性をさらに高められる。

【0025】以上、本発明の実施例を説明したが、これらの実施例は、パッシブダブルスター形光加入者線伝送方式の様に、上り方向は下り方向と違って他の加入者に盗聴される心配が無い様な場合に適している。もし、上り方向の伝送も安全でない場合は、パスワードを通常の秘密鍵暗号方式によって暗号化して送信することによって安全性を保つことができる。この場合、第二の実施例での最初の暗号化されたパスワードの送信の際には、さらなる暗号化は必要ない。このため、パスワード 자체を秘密鍵暗号方式の秘密鍵として使用することもできる。

【0026】

【発明の効果】以上の説明から明らかな如く、本発明によれば、公開鍵暗号化方式の一方向性を利用して、安全性が高くかつ所要回路規模の少ない加入者認証を実現することができる。また、個々の加入者側伝送装置を区別するためのID番号を加入者側伝送装置に設定することにより、暗号化されたパスワードを加入者からの申告によりあらかじめ局側伝送装置に登録しておく代わりに、加入者側伝送装置の設置時に、局側伝送装置からの呼び出しで自動的に遠隔登録することができる。さらに、通信の開始時の加入者側伝送装置の呼び出しにID番号を併せて用いることにより、パスワードを一部のみ使用することが可能となるため、パスワードの安全性をさらに高めることができる。

【図面の簡単な説明】

【図1】本発明の第1の実施例のパスワード登録時の手順を説明する図である。

【図2】本発明の第1の実施例の通信開始時の手順を説

明する図である。

【図3】本発明の第2の実施例のID番号登録時の手順を説明する図である。

【図4】本発明の第2の実施例のパスワード自動登録の手順を説明する図である。

【図5】本発明の第2の実施例の通信開始時の手順を説明する図である。

【図6】従来の加入者認証方式を説明する図である。

【図7】図6の続きを示す図である。

【図8】登録加入者通信サービスシステムの一例の概略構成を示す図である。

【図9】公開鍵暗号方式を説明する図である。

【符号の説明】

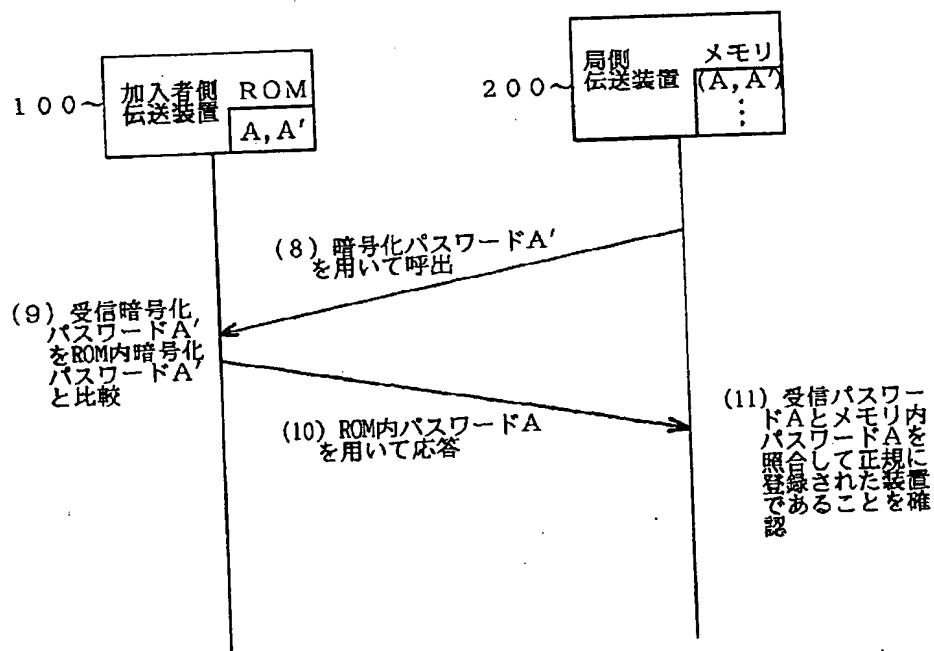
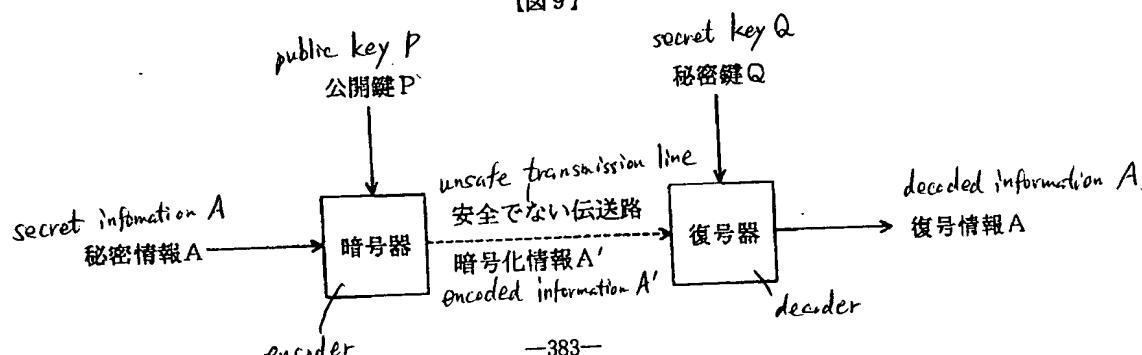
100 加入者側伝送装置

200 局側伝送装置

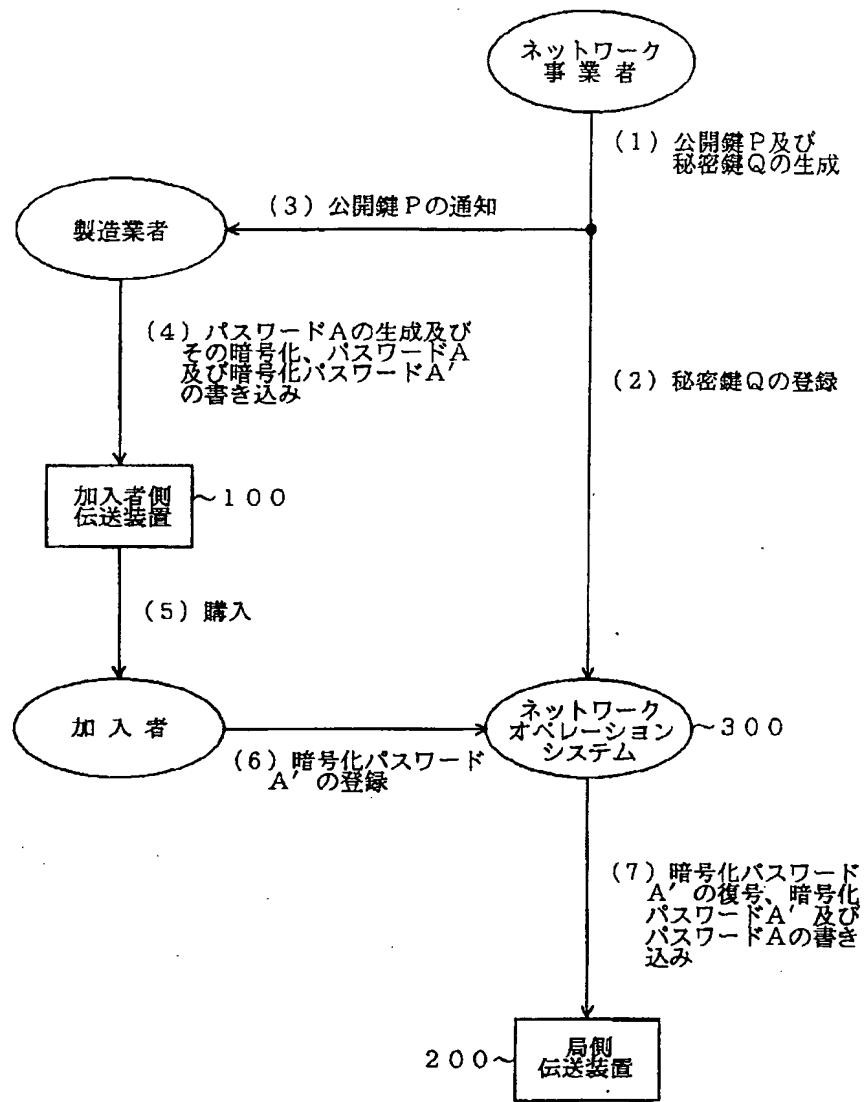
300 ネットワークオペレーションシステム

400 ネットワーク

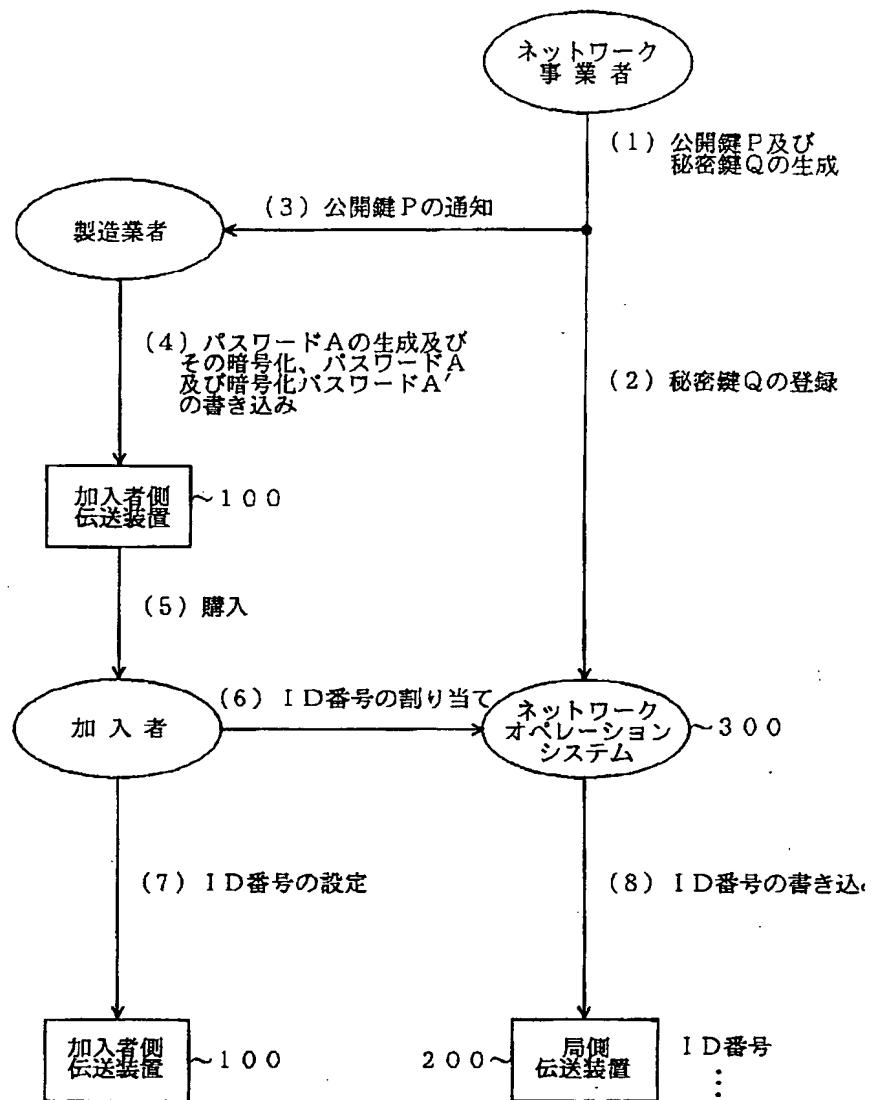
【図2】

Fig. 9
【図9】

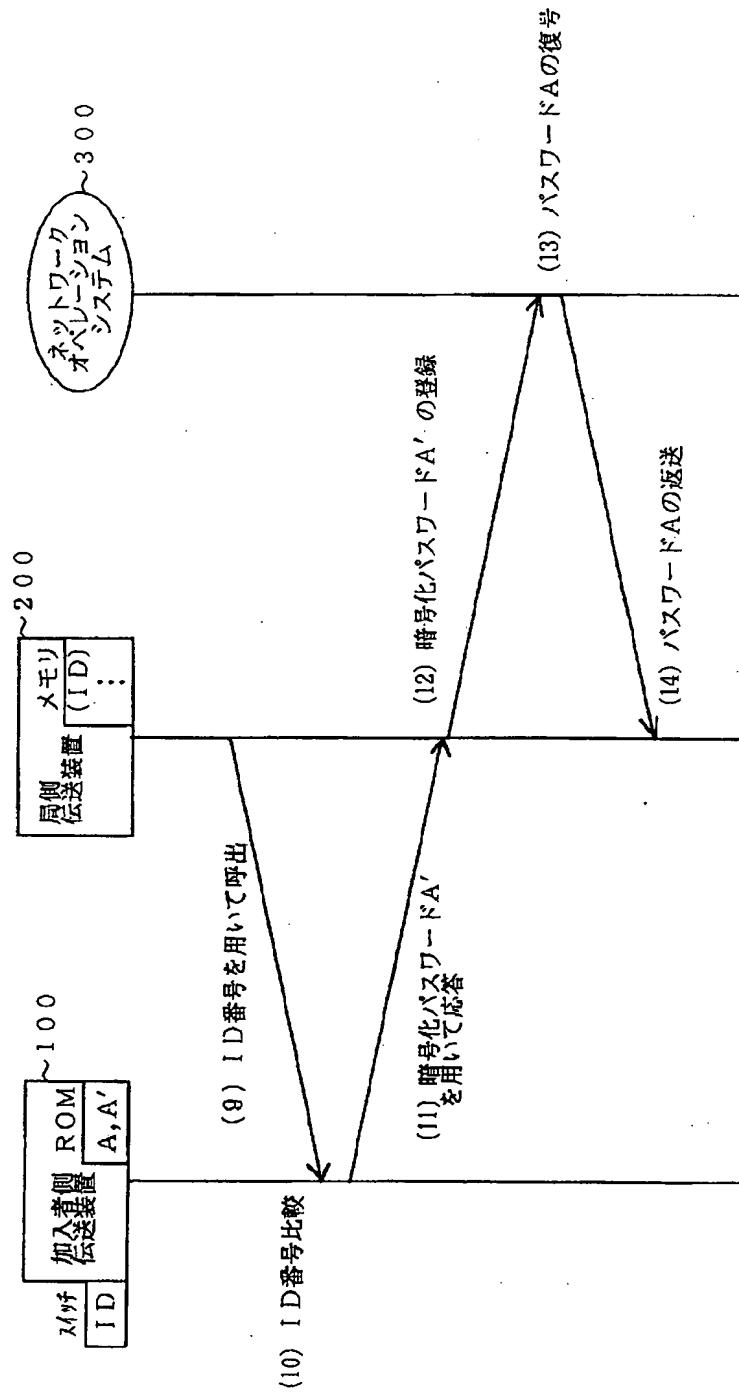
【図1】



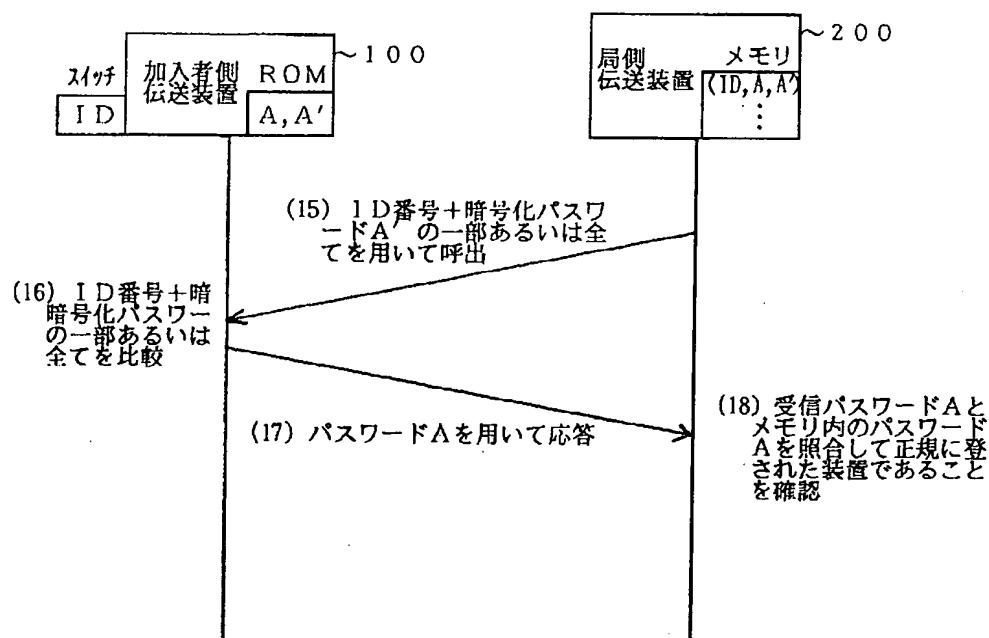
【図3】



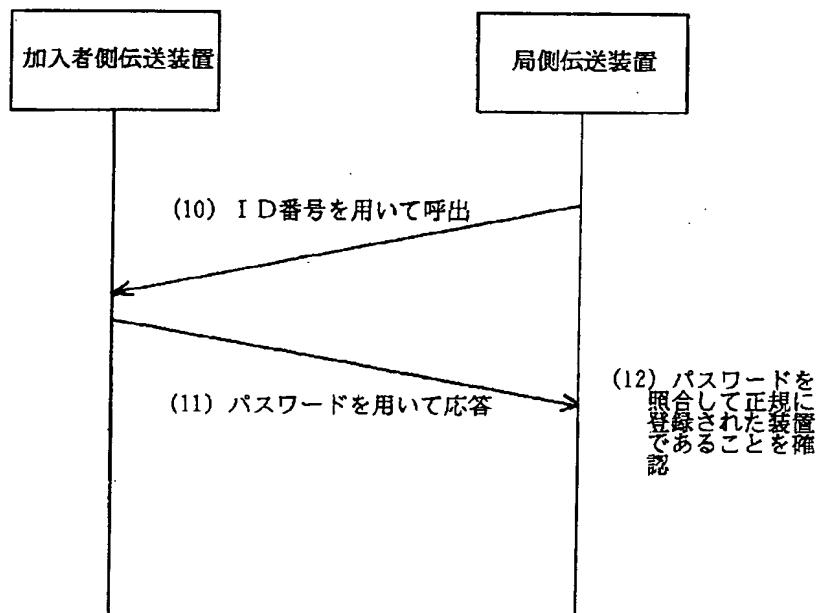
【図4】



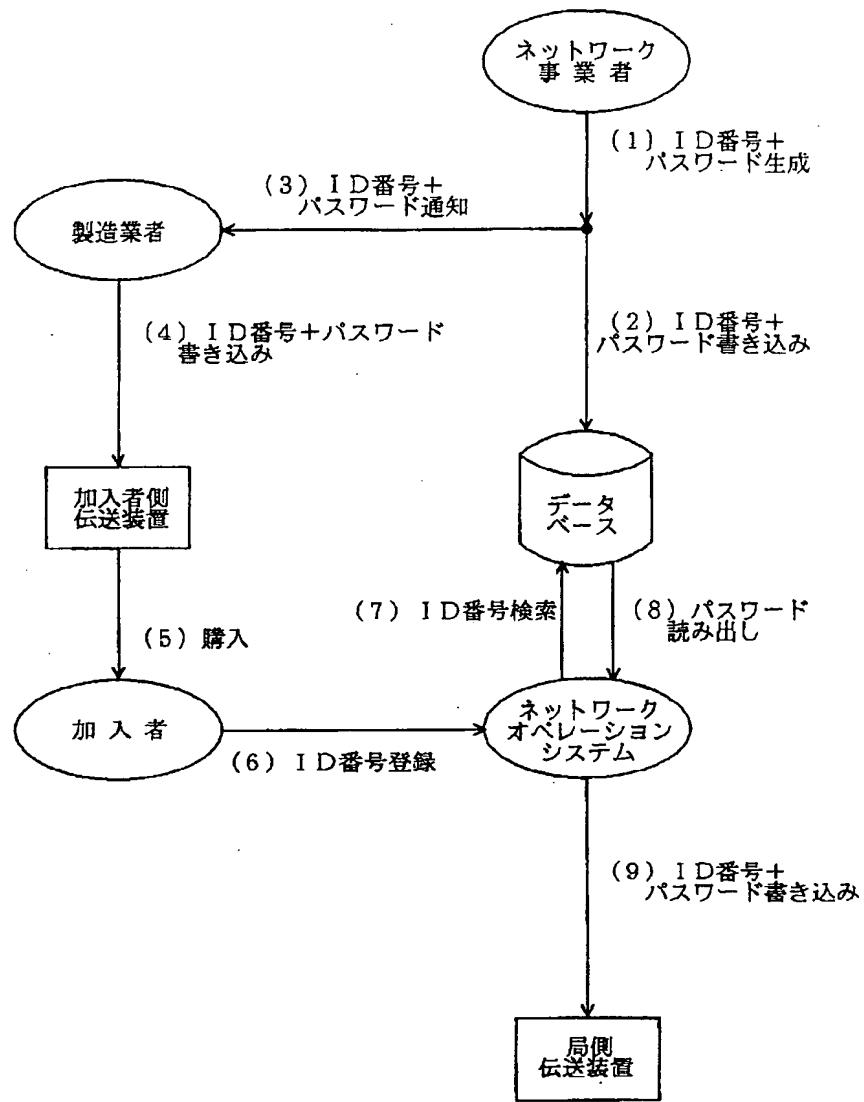
【図5】



【図7】



【図6】



【図8】

